DEPARTMENT OF HOMELAND SECURITY: MISSED DEADLINES – MISSED OPPORTUNITITES TO SECURE AMERICA

July 15, 2005

Prepared by the Minority Staff of the
House Committee on Homeland Security
Representative Bennie G. Thompson, Ranking Member
Representative Kendrick B. Meek, Ranking Member
Subcommittee on Management, Integration and Oversight

DEPARTMENT OF HOMELAND SECURITY
MISSED DEADLINES – MISSED OPPORTUNITIES TO SECURE AMERICA

The Department of Homeland Security was created more than two years ago with the mission of protecting America against terrorism here at home. The Department was tasked with securing our nation's borders, sea ports, skies, critical infrastructure, cyber networks, and our rail and transit systems. It also became our focal point for responding to terrorism attacks and disasters. The Department was our answer to making sure that 9/11 never happened again.

Congress moved quickly to give the new Department the best and most effective tools available to do the job. The Department was designed to bring the 22 agencies with terrorism prevention, detection and response components under one house. The Department has let Congress and the American people down.

Congress has an obligation to ensure that the Department is accountable to the American people for making America as secure against terrorism as possible. At the same time Congress is accountable to the American people for making sure that their tax dollars are spent to truly enhance homeland security. This is why Congress set deadlines for the Department and required it to submit reports on progress on security programs. If measures or deadlines are unreasonable, then the Department must engage Congress as to how to reach better solutions.

Far from being simply summer reading on security issues for Congress, these reports are critical to carrying out the Department's mission. These reports allow Congress and the American people to measure how prepared we are at home. They also provide guidance to Congress on whether or not the Department and other related entities need additional resources or tools in order to accomplish their homeland security mission.

On March 9, 2005, Congressman Kendrick B. Meek (D-FL), Ranking Member of the Management Subcommittee, and I wrote to the Department of Homeland Security Secretary Michael Chertoff expressing our concern about more than 100 deadlines that the Department had let pass without delivering results. To date, we are still awaiting a briefing promised to us by the Department in April. The Democratic Members of the Homeland Security Committee are deeply concerned that no one in the Department appears to have a full accounting of the reports that must be delivered to Congress and a specific accounting of which ones have and which ones have not been delivered. We have requested a summary and have not received a response.

Attached is an abbreviated list of critical reports that remain "missing in action" and an explanation of why it is important that the Department of Homeland Security deliver these reports to Congress.

Sample Missed Deadlines – The following deadlines were unmet as of July 13, 2005.

* Transportation

Port Security

The Department of Homeland Security's port security grant and cargo security programs have been criticized by both the Department's Inspector General and the Government Accountability Office for poor management that has resulted in ineffective security programs and wasted taxpayer dollars. The Administration still has not developed a comprehensive port security plan for the nation's ports. These reports are important to securing our ports.

- Report on Design of Maritime Transportation Security Grant Program (due - November 9, 2004; Section 804, Coast Guard and Maritime Transportation Act of 2004).

- Report on cargo container security (due - February 8, 2005; FY05 Homeland Security Appropriations Act).

- Report on evaluation of cargo inspection targeting system for international cargo containers (due - February 9, 2005; Section 809, Coast Guard and Maritime Transportation Act of 2004).

- Completion of National Maritime Transportation Security Plan (due - April 1, 2005; Section 4072, Intelligence Reform and Terrorism Prevention Act of 2004).

Transportation Security

The Department has repeatedly promised to develop a national strategy to secure the nation's transportation system, including public transit. In light of last year's transit attack in Madrid and the recent attack in London, there is heightened awareness of the need to secure our transportation sector.

- Initial strategy report for National Transportation Security [and modal security plans] (due - April 1, 2005, and annually thereafter; Section 4001, 2004 Intelligence Reform and Terrorism Prevention Act).

* First Responders

DHS continues to miss deadlines on reports related to emergency preparedness and response. Congress created the Rural Domestic Preparedness Consortium to ensure that citizens in rural America are adequately protected. To date, the Department has not delivered a report detailing the creation of this consortium. The Department has also failed to produce a report detailing their emergency housing plan. This plan is vital to ensuring that America can adequately recover from an attack.

- Report on the Emergency Preparedness and Response Directorate's emergency housing plan and its evaluation and deployment of these new housing solutions to the House and Senate Appropriations Committees (due - January 14, 2005; FY05 Department of Homeland Security Appropriations Act).

- Report from the DHS Office of State and Local Government Coordination and Preparedness on the creation of the Rural Domestic Preparedness Consortium (due - January 15, 2005; FY05 Department of Homeland Security Appropriations Act).

- Interim report from the Secretary of DHS regarding the progress of the interagency communications pilot projects (due - June 17, 2005; Section 7304, Intelligence Reform and Terrorism Prevention Act of 2004).

*** Intelligence**

It has been three and a half years since 9/11, and DHS has not yet completed a threat/vulnerability assessment that can drive strategies, set priorities, and guide spending to secure the homeland. Section 7306 of the Intelligence Reform Act required the Secretary to complete such an assessment – as well as both a plan to protect the nation's critical infrastructure and a description of the government's readiness to respond to terrorist threats. Every day past that deadline represents a missed opportunity to protect America.

- IAIP report "Critical Infrastructure Risk Assessment and Readiness" was submitted into the DHS Clearance review process on July 12, 2005 (due – June 17, 2005; Section 7306, Intelligence Reform and Terrorism Prevention Act of 2004).

*** Aviation**

<u>Air Cargo Security</u>

Every year, 2.8 million tons, of the estimated 12.5 million tons of cargo transported, are transported on passenger planes. The risk that undetected explosive and incendiary devices in air cargo space has been a matter of concern since the 1988 downing of Pan Am Flight 103 over Lockerbie, Scotland, that killed 230 passengers.

The Aviation and Transportation Security Act (ATSA) of 2001 requires that all cargo carried aboard commercial passenger aircraft be screened. The Transportation Security Administration was required to have a system in place as soon as practicable to screen, inspect, or otherwise ensure the security of cargo on all-cargo aircraft.

According to a September 2003 report by the Congressional Research Service, less than 5 percent of cargo placed on passenger airplanes undergoes physical screening. TSA touts its "system of systems" layered approach to aviation security. Its failure to move forward in a substantive way to improve cargo security on passenger planes leaves a major gap in our nation's air security systems.

Blast resistant cargo containers that can hold either cargo or luggage could help reduce the risk of a bomb taking down a passenger plane. The Intelligence Reform and Terrorism Prevention Act directs TSA to transmit a report on the effectiveness of blast-resistant cargo containers by June 15, 2005. This report was never transmitted to Congress.

- Report on pilot program findings on blast-resistant cargo and baggage containers (due - June 15, 2005; Section 4051, Intelligence Reform and Terrorism Prevention Act).

- Report on in-bound all-cargo aircraft security (due - June 15, 2005; Section 4054, Intelligence Reform and Terrorism Prevention Act).

Explosives at the Checkpoint

While TSA regularly screens passengers' checked baggage for explosives, their carry-on bags rarely undergo such scrutiny. Equipment currently at use at most of our nation's airports is incapable of detecting a bomb or other incendiary device if it is on a person or in the carry-on bag of a would-be suicide terrorist.

The Fiscal Year 2005 Homeland Security Appropriations Act required TSA to transmit a detailed report on TSA's pilot program to screen passengers and carry-on baggage for explosives, including implementation costs and schedules for purchase, installation, and maintenance of new technologies.

The 9/11 Act required the Department to submit a strategic plan to promote the optimal utilization and deployment of explosive detection equipment at airports to screen individuals and their personal property. Such equipment includes walkthrough explosive detection portals, document scanners, shoe scanners, and backscatter x-ray scanners. The development and implementation of a strategic plan is important for DHS to reduce the risk that a suicide terrorist will carry a bomb or incendiary device on a plane on his body or in his bag.

- TSA report on the Agency's pilot program to screen passengers and carry-on baggage for explosives (due - February 10, 2005; Homeland Security Appropriations Act for Fiscal Year 2005).

- DHS Strategic Plan for Deployment and Use of Explosive Detection Equipment At Airport Screening Checkpoints (due - March 17, 2005; Section 4013, Intelligence Reform and Terrorism Prevention Act).

Deploying Better Aviation Screening Equipment

The 9/11 Act required the Department to "take such action as may be necessary to expedite the installation and use of in-line baggage screening equipment at airports." Integrating the explosive detection system (EDS) machines into baggage systems would prevent passengers from waiting in longer lines at ticket counters where they can create unnecessary security and safety risks. Investing in in-line EDS systems would also improve efficiency. Earlier this

year, the Government Accountability Office concluded that in-line baggage screening systems at the nine airports that have received funds from TSA could net and save the federal government $1.3 billion over seven years compared with stand-alone EDS systems. TSA also indicated that the agency could recover its initial investment in the in-line systems at these airports in a little over one year.

Additionally, the 9/11 Act requires Congress to provide a schedule for replacing trace-detection equipment, as soon as practicable and where appropriate, with EDS equipment. TSA's experience with trace detection equipment has shown it to be inferior to EDS in that it is highly labor intensive and limited in its ability to detect threats.

- DHS Report, including schedule, on installation of in-line baggage screening equipment and replacement of Explosive Trace Detection with Explosive Detection Systems (due - June 15 2005; Section 4019, Intelligence Reform and Terrorism Prevention Act).

Other critical aviation security reports owed to Congress under the Intelligence Reform and Terrorism Prevention Act of 2004.

- Pilot program to deploy and test advanced airport checkpoint screening devices and technology at five airports (due – March 31, 2005).

- Guidance report on integrated biometrics in airport access control systems (due – March 31, 2005).

- Development of law enforcement travel credential (due – April 16, 2005).

- Report on the viability of providing devices or methods, including wireless systems, to enable flight crews to discreetly notify the pilot in the case of a security breach (due – June 15, 2005).

- Report on "human factor improvement" of TSA screener performance (due – June 15, 2005).

- Report on secondary flight deck barriers (due – June 15, 2005).

*** Privacy**

This Department of Homeland Security was required to conduct a 'retro-analysis' of the privacy impact on the American public of the known or suspected terrorists lists that were established for the purpose of keeping such individuals off commercial flights. Given the revelation that TSA did not comply with the Privacy Act of 1974 when it began testing its new Secure Flight program, the privacy implications of the Automatic Selectee and No-Fly Lists have gained renewed prominence. If TSA is unable to get Secure Flight off the ground, privacy issues will need to be addressed concerning the lists created to support it. An assessment of how well the lists comply with applicable law, and what mechanisms are or

should be in place to correct errors, may well inform TSA's new passenger screening initiatives going forward.

- DHS Privacy Officer Report on Impact of the Automatic Selectee and No-Fly Lists on Privacy and Civil Liberties (due - June 15, 2004; Section 4012 of the Intelligence Reform and Terrorism Prevention Act of 2004).

*** Critical Infrastructure Protection**

The National Asset Database is still filled with low-priority targets and inaccurate information. Congress requested the following report to check on the methodology and progress of the NAD, in order to help assure we created a comprehensive list of the nation's assets.

- Report on critical infrastructure vulnerabilities and risk assessments (due – June 17, 2005; Sec. 7306, 2004 Intelligence Reform and Terrorism Prevention Act).

This is probably the most important item in Critical Infrastructure Protection. The National Infrastructure Protection plan is the overall roadmap of department policy for protection our critical infrastructure and national assets. The fact that it is 7 months overdue demonstrates that the Administration has not made Critical Infrastructure Protection a priority.

- The Final National Infrastructure Protection Plan (due - December 17, 2004; Homeland Security Presidential Directive 7) is still in "Interim" Status, which was released in Feb 2005.

Several of the contracts that DHS has entered have been sole-sourced. Congress must conduct proper oversight to ensure that federal funds are being wisely spent. DHS should help in this effort by providing this report.

3) Quarterly Sole-Source Contract Agreements Report by IAIP Under Secretary (due - January 31, 2005; FY05 Homeland Security Appropriations Act).

*** Border Security**

The lack of sufficient information sharing hampers the ability of our border agents to adequately carryout their mission to protect the border. This could result in a terrorist suspect or criminal alien freely moving through interior border checkpoints. As such, it is vital that this study is completed to provide assurance that there are no weaknesses in the sharing of information among and between our border inspection agencies. This includes interoperability and the ease at which these agencies can readily communicate.

- Report on sharing of information between border inspection agencies (due - May 25, 2003; Sec. 427, Homeland Security Act of 2002).

This comprehensive review is needed to ensure that the provisions of the Immigration and Naturalization Act are being fully addressed in a post-911 environment and that CBP and ICE are focused on the proper priority of protecting the homeland as well as the rights and interest of those who wish to travel to and visit our nation.

- Report detailing how Bureau of Border Security [now CBP and ICE] will enforce all the enforcement provisions of the Immigration and Naturalization Act relating to such functions (due January 24,2004; Section 445, Homeland Security Act of 2002).

This report is critical to national/homeland security and needed to ensure that DHS has fully assessed the adequacy and weaknesses with the integrated entry and exit data system that is part of the US-VISIT program for protecting the homeland against terrorist suspects and criminal aliens entering the country. Without an adequate integrated entry and exit program, DHS is not capable to fully identify and prevent those attempting to enter or already in the U.S.

- Report on the implementation of the integrated entry and exit data system (due – December 31st of each year; Section 110 (e) (1), Illegal Immigration Reform and Immigrant Responsibility Act of 1996).